*Brincar, estudar e...*
*navegar com segurança na Internet!*

# Sumário

# CARTA DE APRESENTAÇÃO

O governo federal, com a coordenação da Subsecretaria de Promoção dos Direitos da Criança e do Adolescente/Secretaria Especial dos Direitos Humanos da Presidência da República, desenvolve um conjunto de ações visando o enfrentamento da violência sexual contra crianças e adolescentes. Uma das principais iniciativas é o Disque Denúncia Nacional - DDN 100, que serve como um importante canal de comunicação da sociedade civil com o poder público, visando proteger as crianças e adolescentes e também responsabilizar os agressores. Este Serviço também desenvolve metodologias de recebimento e encaminhamento de denúncias que tem servido de suporte para a rede de canais locais de denúncias.

Em 2008, uma nova parceria foi estabelecida usando um outro meio, a Internet, para mobilizar a sociedade para denúncias de pornografia infantil neste ambiente. A Secretaria Especial dos Direitos Humanos e o Ministério da Justiça, com apoio da Petrobrás, firmaram acordo com a Safernet para desenvolvimento do hotline federal para o rastreamento destes sites. Também faz parte deste projeto a disseminação de procedimentos para navegação segura na Internet, em especial voltados para crianças e adolescentes, famílias e educadores.

A publicação da presente cartilha, elaborada pela equipe da Safernet Brasil, compõe este conjunto de ações, que serão articuladas com o Ministério da Educação, tendo como objetivo desenvolver vários instrumentos de educação e comunicação para o empoderamento da população sobre o uso da Internet e os cuidados diante de sites que contenham mensagens violadoras dos direitos de crianças e adolescentes, em especial de pornografia infantil.

Destaca-se ainda a particularidade do momento histórico de publicização desse documento, visto que em 2008 comemoramos os 60 anos da Declaração Universal dos Direitos Humanos, os 18 anos do Estatuto da Criança e do Adolescente – ECA e a realização do III Congresso Mundial de Enfrentamento da Exploração Sexual de Crianças e Adolescentes onde esta cartilha será distribuída. Tais eventos constituem um momento ímpar de repactuação social no sentido de reafirmar que a proteção da infância e adolescência brasileira é dever de todos os brasileiros e de todas as brasileiras. Assim sendo, esperamos que a experiência apresentada indique possibilidades nesse caminho.

Carmen Oliveira
Subsecretaria de Promoção dos Direitos da Criança e do Adolescente.

# SaferNet Brasil

A SaferNet Brasil é uma associação civil sem fins lucrativos e econômicos, sem vinculação político-partidária, religiosa ou racial, fundada em 20 de dezembro de 2005, por um grupo formado por cientistas da computação, professores universitários, pesquisadores e bacharéis em Direito.

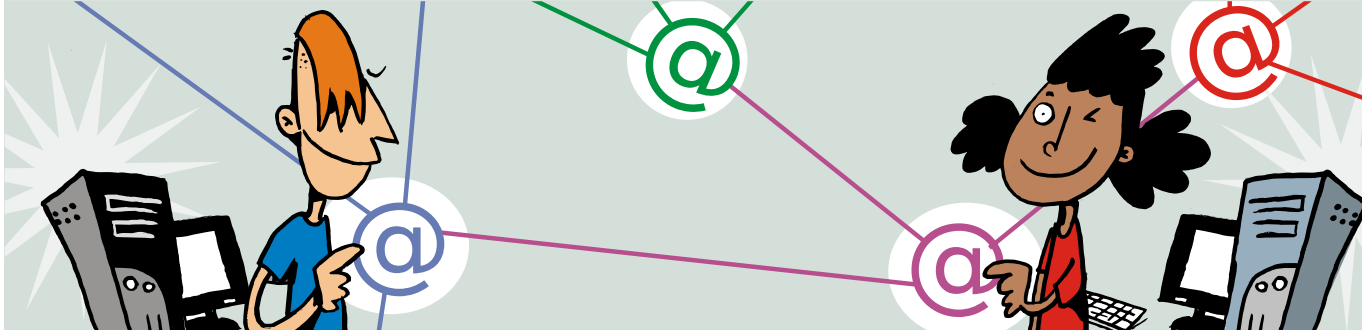
A SaferNet Brasil criou e mantém a Central Nacional de Denúncias de Crimes Cibernéticos (www.denunciar.org.br) que, desde 29/03/2006, é operada em parceria com o Ministério Público Federal. Reconhecida e recomendada pelo poder público como único hotline da América Latina e Caribe, a Central oferece o serviço gratuito de recebimento, processamento, encaminhamento e acompanhamento online de denúncias anônimas sobre crime ou violação aos Direitos Humanos praticado por meio da Internet.

A Central Nacional de Denúncias de Crimes Cibernéticos recebe uma média de 2.500 denúncias (totais) por dia envolvendo páginas suspeitas de conter evidências de crimes de Ponografia Infantil, Racismo, Neonazismo, Intolerância Religiosa, Apologia e/ou Incitação a crimes contra a vida, Homofobia e Maus tratos contra os animais.

A SaferNet Brasil também desenvolve um conjunto de ações focadas na área de Prevenção de Crimes e Violações aos Direitos Humanos na Internet. A SaferNet Brasil entende que atuar na prevenção é uma forma eficaz para reduzir a incidência de atos ilícitos no ciberespaço. Do mesmo modo, reconhece que a complexidade do problema exige medidas permanentes de combate, educação e conscientização.

Sabemos que a Internet é uma ferramenta fantástica, que pode contribuir muito com o desenvolvimento cognitivo, social e emocional de nossas crianças. Porém, como toda tecnologia que se propõe a aproximar pessoas, também pode colocar em risco a segurança e a saúde de crianças, jovens e adultos, quando não orientados sobre o uso ético e responsável da rede. Por essa razão, o uso da Internet pelas crianças e adolescentes precisa ser estimulado conjuntamente com ações efetivas de orientação e acompanhamento dos pais e educadores.

Conheça mais sobre as nossas ações: www.safernet.org.br

Se você testemunhou algum crime na Internet, denuncie: www.denuncie.org.br

# Internet

Rede de milhões de computadores de todo o mundo interligados por linhas telefônicas, fibra ótica e satélites. Além de ligar redes de computadores, conecta milhões de pessoas que formam suas redes de relacionamento e navegam pelas informações disponíveis no espaço virtual, também chamado de Ciberespaço. Cada vez mais será comum usar o celular para navegar na Internet.

## Aproveite!

- Acesso e troca de diferentes tipos de materiais como imagens, sons, vídeos e textos;
- Permite a comunicação e amizade entre pessoas de qualquer lugar do mundo;
- Rica fonte para estudos, pesquisas, trabalho e diversão;
- Supera limites de tempo e espaço, criando um novo espaço público, o ciberespaço.

## Cuidado!

- Pode ser prejudicial se usada sem limites ou quando substitui todas as outras atividades de lazer;
- Como todo espaço público, pode ser acessada por pessoas mal intencionadas;
- A Internet não é "terra sem lei". Apesar da sensação de anonimato, quem praticar crime por meio dela pode ser identificado e punido;
- Não podemos confiar em todas as informações, nem em todas as pessoas conectadas;
- Proibir não educa nem previne. Dialogue e busque orientação.

## Dicas para manter-se seguro

- Nunca divulgue senhas, nome completo, endereços, números de telefone ou fotos íntimas;
- Você distribui qualquer foto sua no mural da escola, no ônibus ou na praia? Porque então divulgar na Internet? Pense bem antes de publicar algo. Uma vez na rede, é quase impossível controlar o uso;
- Comunique-se com educação. Respeito deve valer em qualquer espaço e com qualquer pessoa, mesmo com aquelas que não conhecemos;
- Evite gravar as senhas e login no computador para não facilitar roubos;
- Cuidado ao baixar arquivos, eles podem conter vírus, materiais impróprios ou serem ilegais. Anti-vírus e filtros podem ajudar a proteger;
- Nunca aceite que sites instalem programas em seu computador e não faça download de nada que você não saiba exatamente o que é e de onde vem;
- Busque provedores e serviços que ofereçam recursos de segurança, que sejam éticos e responsáveis;
- Dialogue sempre com amigos, filhos e professores para se manter informado sobre segurança na Internet;
- Se precisar de ajuda para tirar suas dúvidas, envie e-mail para prevencao@safernet.org.br

# Navegadores ou Browsers

Programas que permitem visualizar os conteúdos e "surfar" pelas páginas na Internet. Os mais conhecidos são o Mozilla Firefox e o Internet Explorer.

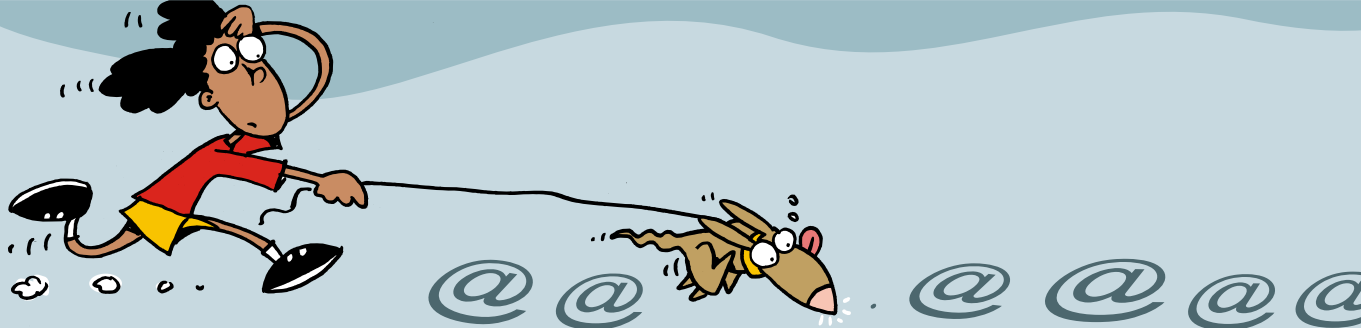
## Aproveite!

- Uso simples e dinâmico para navegar na Internet;
- Permitem ajustes para apagar senhas, filtrar sites e copiar páginas;
- Ajudam a guardar os endereços para voltar aos sites preferidos.

## Cuidado!

- Geralmente não identifica sozinho páginas falsas ou ilegais;
- O usuário é quem define o que visitará. No programa tudo pode ser visto;
- Cuidado com os sites ilegais e com conteúdos impróprios para crianças;
- O navegador não garante sozinho a segurança de informações pessoais, senhas e dados bancários.

## Dicas para manter-se seguro

- Sempre leia com atenção as mensagens mostradas pelo navegador, pois elas podem ajudar a identificar um programa malicioso ou um site falso;
- Não autorize instalação de software de desconhecidos ou de sites estranhos;
- Use o bloqueio de pop-up em seu navegador;
- Quando digitar um endereço, confirme se o que está na tela é exatamente o que procurava;
- Atenção com transações financeiras via Internet. Quando fizer, confira se aparece o desenho de um "cadeado fechado" no rodapé da página e se o endereço começa com https, em vez de http;
- Dê preferência aos navegadores de Internet livres que são mais seguros, a exemplo do Mozilla Firefox, Epiphany , Konqueror
- Em caso de visualizar conteúdos suspeitos de violarem os Direitos Humanos, denuncie em www.denuncie.org.br e bloquei o endereço.

# Sites de Busca

São páginas que oferecem o serviço de busca de conteúdos disponíveis em outros sites na Internet a partir de expressões ou palavras-chave. Em geral, os sites de busca são gratuitos e apontam outros endereços onde é possível encontrar o conteúdo buscado. Exemplo: Google, Bing, Yahoo...

## Aproveite!

- Permitem pesquisas rápidas em quase todo conteúdo da Internet entre fotos, vídeos, textos, livros, músicas, imagens, programas etc;
- Os maiores são gratuitos e atualizados a todo instante;
- Facilitam achar o que queremos na imensidão do ciberespaço.

## Cuidado!

- Podem apresentar conteúdos indesejados ou diferentes do procurado;
- Geram resultados de acordo com as palavras-chave, mesmo quando escritas de forma errada;
- Geralmente exibem o resultado da busca baseado na popularidade, e não na relevância;
- Mesmo os conteúdos ilegais podem ser encontrados nas buscas;
- Crianças podem facilmente encontrar conteúdos agressivos e impróprios.

## Dicas para manter-se seguro

- Não confie em tudo o que vê ou lê, muitos conteúdos são falsos e mentirosos;
- Os sites de busca não substituem as bibliotecas, estimule a leitura. Na biblioteca, também pode ser legal navegar;
- Para evitar resultados muito amplos, coloque as palavras entre aspas (" ");
- Feche as páginas que não estão relacionadas ao assunto esperado para evitar constrangimento;
- Use o serviço de pesquisa segura (Safe Search) dos buscadores. Procure em preferências e ative a filtragem de páginas com conteúdo sexual explícito, impedindo que elas apareçam nos resultados da pesquisa;
- Em caso de visualizar conteúdos suspeitos de violarem os Direitos Humanos, denuncie em www.denuncie.org.br

# LAN House e InfoCentro

São centros públicos de acesso à Internet com vários computadores em rede. Os Infocentros e Telecentros são espaços criados e apoiados pelos governos para ampliar o acesso gratuito à Internet no País. A diferença entre eles e as Lan Houses (ou Cibercafés) é que as Lan Houses são comerciais e cobram pelo acesso. No Brasil, em 2008, cerca de 48% dos internautas brasileiros acessaram a Internet por meio de uma Lan House. Entre os jovens internautas de 10 a 15 anos, este número sobe para 63%, segundo dados de pesquisa do NIC.br - set/nov 2008.

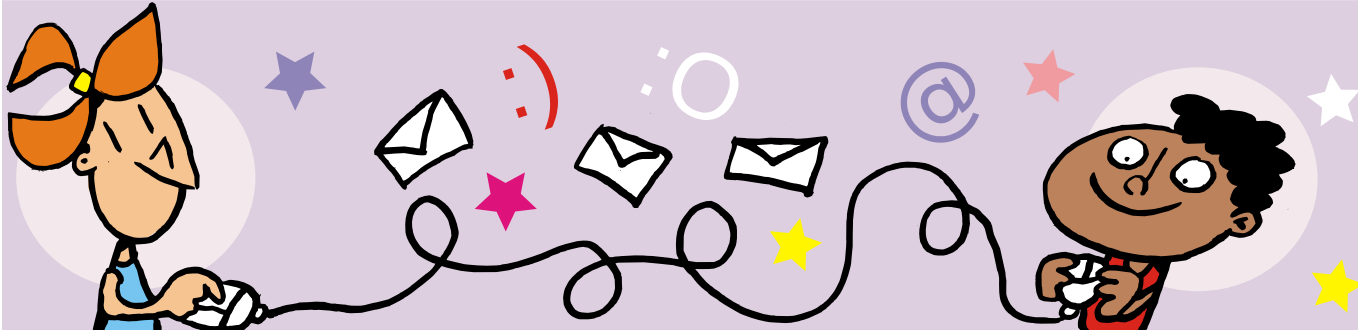
## Aproveite!

- Facilitam o acesso à Internet para quem não tem computador ou não dispõe de conexão com a Internet;
- Permite o acesso à Internet para quem está longe de casa;
- Disponibilidade de diferentes pontos de acesso nos bairros para estudar, jogar, conversar e pesquisar.

## Cuidado!

- Algumas cidades e alguns Estados exigem autorização para acesso de crianças desacompanhadas;
- Quando não há exigência de identificação ou cadastro, pode ser aproveitada para esconder pessoas mal intencionadas ou que praticam crimes pela Internet;
- O acesso sem orientação adequada pode colocar as crianças e adolescentes em risco;
- Nem sempre o ambiente é próprio para meninos e meninas, conheça os responsáveis pelo espaço.

## Dicas para manter-se seguro

- Lembre sempre de clicar em "sair" antes de fechar as páginas e os programas;
- Atenção para não deixar suas senhas gravadas;
- Use somente o tempo necessário para evitar desperdício de tempo e dinheiro;
- Não aceite ajuda de estranhos e chame sempre o responsável em caso de dúvida;
- Evite acessar bancos e fazer compras pela Lan House e Infocentros;
- Se precisar de ajuda para tirar suas dúvidas, envie e-mail para prevencao@safernet.org.br

# e-Mail

Serviço de troca de mensagens e "cartas" oferecido pela Internet que permite enviar e receber textos, imagens, apresentações e quase todo tipo de informação em formato digital. A comunicação não é simultânea, você envia e recebe as mensagens por meio de uma caixa postal que fica em um dos computadores interligados à Internet. Para conferir suas novas mensagens, é preciso entrar periodicamente em sua caixa postal na Internet. Os endereços de e-mail são sempre identificados com @ entre os nomes. Exemplos: voce@safernet.com.br (acentos não são aceitos)

## Aproveite!

- Muitos são gratuitos e permitem que todos tenham sua própria "caixa postal" na Internet;
- Facilita a troca de textos, fotos e vídeos entre as pessoas de todo o mundo;
- Agiliza a comunicação, pois as mensagens levam apenas alguns instantes para chegar ao destino com pouco custo, independentemente da distância.

## Cuidado!

- Pode haver muitas informações falsas e golpes nas mensagens;
- Criminosos podem se aproximar para prejudicar, difamar e roubar;
- Crianças podem receber conteúdos impróprios e até serem aliciadas;
- Método mais utilizado para espalhar vírus;
- Atenção àquelas propostas boas demais ou produtos milagrosos, pois geralmente são fraudes.

## Dicas para manter-se seguro

- Você pode configurar sua conta para bloquear contatos indesejados;
- Troque sua senha periodicamente;
- Não aceite nem abra e-mail de desconhecidos! Simplesmente apague sem ler;
- Procure saber a origem da informação e se o responsável é de confiança ou conhecido;
- Atenção com cartões virtuais. Não abra quando o nome do arquivo tiver .exe no final.
- Evite mostrar seu endereço, número pessoal e outros detalhes. Seja genérico;
- Atualizar o anti-vírus e usar anti-spam pode ajudar;
- Jamais acredite em pedidos de pagamento, correção de senhas ou solicitação de qualquer dado pessoal por e-mail. Comunique-se por telefone com a instituição que supostamente enviou o e-mail e confira o assunto;
- Quando receber mensagens agressivas e com conteúdo impróprio, denuncie em www.denuncie.org.br e/ou chame um adulto de confiança;
- Para denunciar Spam vá ao www.antispam.br/;
- Veja mais dicas e tire dúvidas no www.safernet.org.br/prevencao

# Chat - Salas de Bate Papo

Comunicação em tempo real que ocorre por meio de salas virtuais. Permite troca instantânea de mensagens entre várias pessoas. Geralmente são abertas e todos podem ver, em tempo real, a conversa completa na mesma tela. São conhecidas como Salas de Bate Papo e são divididas por temas, idade ou preferências.

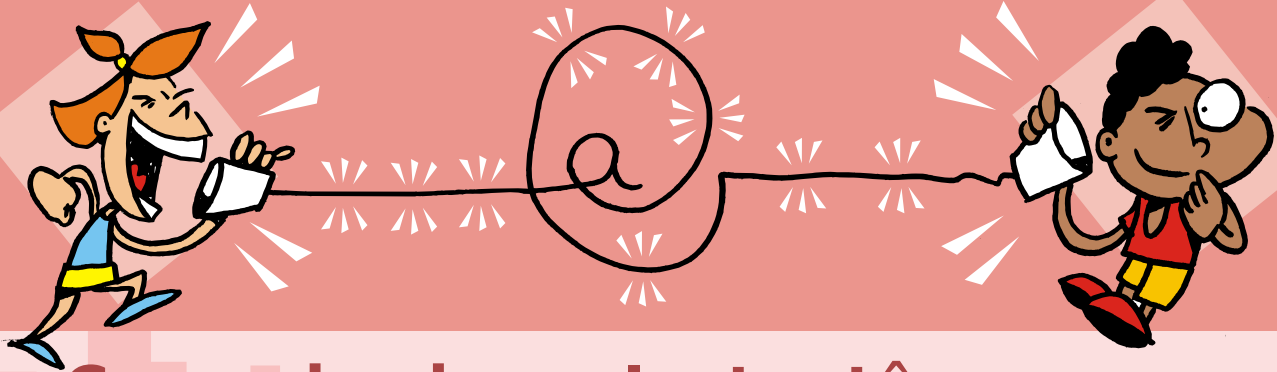
## Aproveite!

- Permite conhecer e conversar "ao vivo" com pessoas de qualquer lugar do mundo;
- Facilita o compartilhamento de idéias e a realização de debates pela Internet;
- Estimula a escrita e leitura para participar das discussões;
- Pode contribuir com a socialização e desenvolver habilidades de comunicação.

## Cuidado!

- As salas são espaços públcos abertos a qualquer um. Precisamos ser educados e tomar cuidado com estranhos;
- As pessoas podem fantasiar e mentir para tentar ganhar confiança e prestígio;
- Em muitas salas, as conversas são impróprias para crianças que podem entrar sem serem identificadas;
- Os apelidos dificultam a identificação e facilitam a prática de crimes.

## Dicas para manter-se seguro

- Não exiba seu nome completo, telefones, endereço, nem lugares que frequenta;
- Jamais encontre "amigos virtuais" sem autorização;
- Tempo de conversa não garante a confiança nem a veracidade das informações, tome cuidado;
- Caso receba mensagens ou imagens agressivas que tentem forçar uma conversa, bloqueie o usuário, denuncie e peça ajuda;
- Em caso de visualizar conteúdos suspeitos de conterem violarem os Direitos Humanos, denuncie em www.denuncie.org.br
- Se precisar de ajuda para tirar suas dúvidas, envie e-mail para prevencao@safernet.org.br

# Comunicadores Instantâneos

São chamados também de Instant Messangers ou Mensageiros Instantâneos. São programas para enviar e receber mensagens simultaneamente. Basta ter um programa e adicionar o endereço de pessoas que usem o mesmo programa para se comunicar em tempo real por meio de texto, voz e/ou vídeo. As conversas podem ser feitas entre duas ou mais pessoas em ambiente privado, diferentemente dos Chats que geralmente tem ambientes abertos para todas as pessoas conectadas. Exemplos de programas gratuitos: MSN, ICQ, Yahoo Messenger, Google Talk.

## Aproveite!

- Permite a comunicação em tempo real, independentemente da distância entre as pessoas conectadas;
- Você pode configurar sua conta para bloquear contatos indesejados e se comunicar apenas com conhecidos;
- Uma vez conectado à Internet, você pode conversar com amigos e parentes distantes sem custos.

## Cuidado!

- Se abrir sua câmera ou enviar fotos para desconhecidos, suas imagens podem ser manipuladas para te prejudicar;
- Pessoas mal intencionadas se passam por " amigos virtuais" e mentem para seduzir, intimidar e ofender outros internautas;
- As imagens da webcam podem mostrar cenas violentas e impróprias;
- Os arquivos trocados por meio das mensagens podem conter vírus.

## Dicas para manter-se seguro

- Não aceite convite de estranhos, prefira se comunicar com quem conhece;
- Não envie fotos pessoais, nome completo, telefones, nem endereços nas conversas com novos amigos;
- Nunca abra a sua webcam para desconhecidos. A webcam pode colocar um estranho mal intencionado dentro de sua casa, cuidado;
- Você distribui convites na rua para estranhos visitarem sua casa? Não faça o mesmo na Internet!
- Evite gravar sua senha e não autorize entrada automática no computador, principalmente se usar em Lan House, Infocentro, ou qualquer local de acesso público;
- Cuidado com os arquivos que recebe, pode ser algo agressivo ou mesmo ilgeal;
- Quando receber arquivo ou mensagem que te ofenda, peça ajuda para gravar, denunciar e bloquear o contato em sua lista.

# Redes de Relacionamento

São sites que permitem criar uma página pessoal na Internet, encontrar amigos, participar e criar comunidades para compartilhar gostos e idéias. Possibilitam atualizar e divulgar um espaço pessoal na Internet com textos, fotos e vídeos. Hoje é um dos espaços preferidos pelos Internautas brasileiros de todas as idades para se encontrarem e se relacionarem pela Internet. Exemplos: Orkut, Twitter, MySpace, Hi5, Facebook...

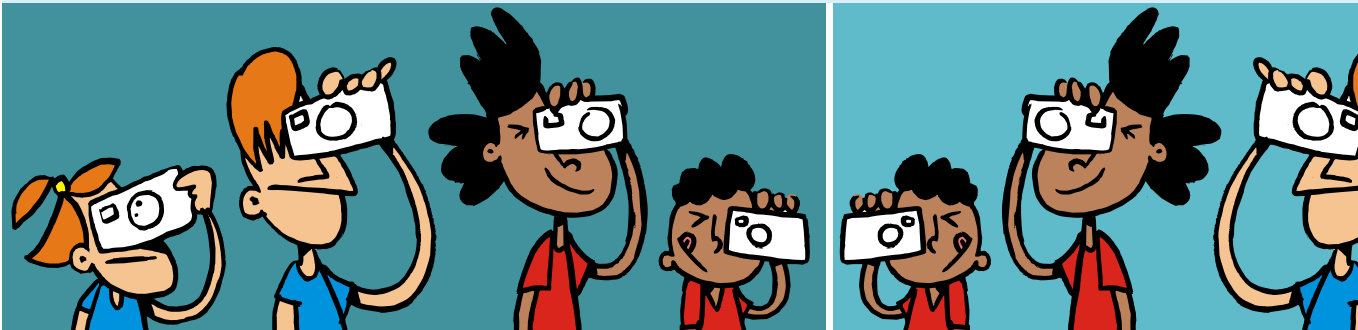
## Aproveite!

- Popularizou a criação de páginas pessoais na Internet;
- Facilidade para reencontrar e aproximar amigos e parentes distantes;
- Facilita o encontro de pessoas com idéias e preferências comuns;
- Permite discussões e debates com liberdade para expressão de temas variados;
- Fornece muitos recursos para divulgar e trocar imagens, vídeos, sites e recados.

## Cuidado!

- Quando divulgamos informações pessoais na Internet, elas se tornam públicas;
- Após publicar algo na Internet, é impossível voltar a escondê-lo;
- Não exponha detalhes de sua vida. Sua intimidade é preciosa e não deve ser aberta para qualquer um;
- Os "cadeados" e bloqueios de acesso podem ser "quebrados" por pessoas mal intencionadas;
- Podem ser usadas para reunir pessoas com intenção de praticar crimes;
- Seus dados podem ser roubados e manipulados para ofender e mesmo chantagear.

## Dicas para manter-se seguro

- Mantenha o mínimo de informações em seu perfil;
- Você distribui seu endereço, suas fotos e telefones para qualquer um na praia, na praça, no ônibus ou no mural da escola? Por que você distribuiria na Internet?
- Não comente sobre detalhes de horários e lugares onde estará. Faça isto por telefone ou por e-mail apenas com quem conhece pessoalmente;
- Se divulgar fotos, use as que não facilitem seu reconhecimento nem endereços ou nome de escola;
- O que importa é a qualidade e não a quantidade de amigos. Cuidado com estranhos;
- Jamais aceite convite de encontro presencial com quem não conhece;
- Troque sua senha periodicamente;
- Caso seja agredido por estranhos, configure sua conta para bloquear os contatos indesejados;
- Se visualizar conteúdos suspeitos de serem racistas ou com cenas de violência contra crianças denuncie em www.denuncie.org.br

# Blogs, Fotologs e Microblogs

São espaços na Internet que podem ser criados por qualquer internauta para publicar suas idéias, fotos, preferências, desejos e expectativas. Nos Blogs e Fotoblogs, podemos debater diversos temas, fazer comentários, enquetes, compartilhar links e todas informações que consideramos interessantes. Podem ser individuais ou coletivos, e geralmente são gratuitos. Os Fotologs são mais dedicados a fotos.

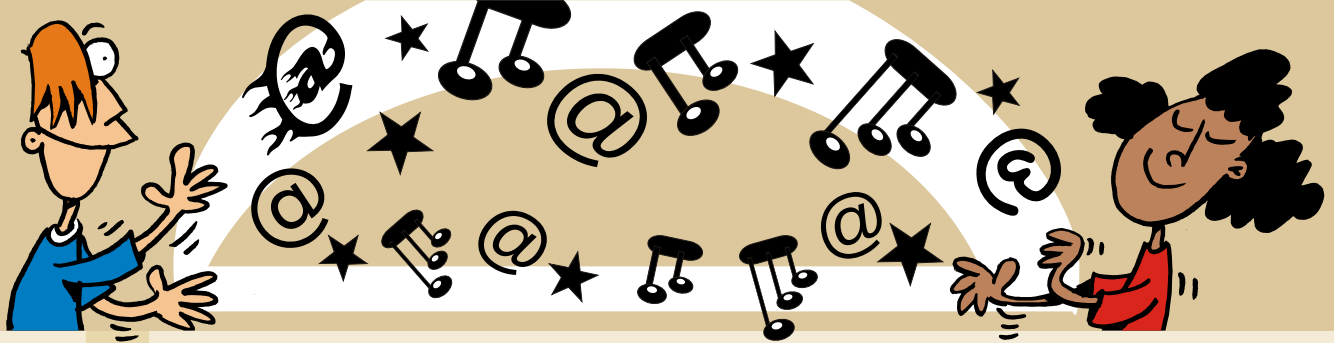
## Aproveite!

- Permitem qualquer pessoa ter um espaço na Internet;
- Ampliam a liberdade de expressão e facilitam a troca de informações entre as pessoas de todo o mundo;
- Estimulam a leitura, a escrita e a criatividade;
- O uso é simples e podem ser atualizados a qualquer momento com muita rapidez;
- As pessoas podem interagir comentando idéias e publicações.

## Cuidado!

- Quando publicamos algo, não podemos mais esconder. Qualquer um pode ver, gravar e usar sem nosso controle. Pense muito bem antes de publicar algo;
- As informações podem ser mal interpretadas e usadas contra você por pessoas mal intencionadas;
- Os comentários podem ser violentos e desrespeitosos;
- Lembre-se de que você é responsável legalmente por tudo o que publica.

## Dicas para manter-se seguro

- Seja educado e cordial também na hora de publicar ou comentar;
- Evite colocar endereço, telefone, nome da escola e nome completo;
- Muito cuidado ao divulgar seus desejos, segredos e sonhos. Sua Intimidade é muito valiosa, cuide bem dela;
- Você colocaria seu diário na praça pública, no mural do colégio ou na praia? Pense muito bem antes de publicar algo na Internet;
- Cuidado com as fotos que posta, elas podem ser modificadas e usadas contra você;
- Você pode usar a moderação dos comentários para evitar mensagens fora do contexto de seu Blog;
- A qualquer momento, você pode apagar seu Blog ou Fotolog mas, uma vez publicado, tudo pode ser gravado por outros e voltar ao ar.

# Redes P2P

Conhecida como P2P (do inglês, peer-to-peer= ponto-a-ponto), é uma rede descentralizada de compuatdores que podem trocar entre si informações como músicas, vídeos, textos e programas. Os usuários das redes P2P fornecem e recebem dados ao mesmo tempo, ou seja, são servidores e clientes simultaneamente. Exemplo: Emule, rede Torrent Além das redes P2P, há os sites de compartilhamento de arquivos. Livros, filmes, fotos e músicas ficam disponíveis em páginas na Intenet para que os internautas possam assistir e em alguns casos gravar. Exemplo: YouTube - visualização de vídeos, RapidShare - compartilhamento de arquivos.

## Aproveite!

- Agilidade incrível para trocar arquivos com outros internautas;
- Não depende de um servidor que controle os dados;
- Permite compartilhar seus conteúdos preferidos e adquirir outros.

## Cuidado!

- Você pode receber arquivos impróprios e agressivos sem desejar;
- Os arquivos podem ter nomes falsos para disfarçar conteúdos ilegais;
- Pode facilitar invasão do seu computador para roubo de dados.

## Dicas para manter-se seguro

- Faça buscas com cuidado e confira o nome e a origem dos arquivos;
- Leia com atenção o contrato de uso dos programas e não permita a divulgação de seus dados pessoais;
- Muito cuidado ao baixar arquivos que sejam executáveis (.exe) ou compactados;
- Busque informações sobre a permissão para gravar e divulgar os arquivos disponíveis na rede;
- Caso receba por engano conteúdos agressivos e que contenham agressões contra crianças, adolescentes, racismo ou intolerância religiosa, denuncie no www.denuncie.org.br

# Jogos On-Line

São jogos que permitem a interação de vários participantes ao mesmo tempo conectados pela Internet. Podem ser jogos de diferentes tipos com ação em equipe e conversas entre os jogadores por meio de mensagens e chat. Alguns jogos podem durar meses e, cada vez que se conecta, o usuário pode continuar de onde parou.

## Aproveite!

- Ajudam a desenvolver habilidades de coordenação motora, estimulam a criatividade e incentivam a leitura;
- Permitem interação com jogadores em diferentes lugares do mundo;
- Podem ser divertidos e educativos.

## Cuidado!

- Jogar em excesso prejudica a saúde e os estudos, podendo até viciar;
- Há pessoas que fingem ser jogadores para prejudicar outras e roubar dados;
- Alguns estimulam a violência e práticas criminosas;
- Há jogos que começam gratuitos e depois cobram taxas por mensagens de celular ou cartão de crédito para continuar.

## Dicas para manter-se seguro

- Não aceite provocações e disputas que possam trazer problemas na "vida real";
- Verifique sempre a idade mínima indicada para cada jogo;
- Na Lan House, verifique se saiu corretamente do jogo para evitar que roubem sua senha;
- Quando receber mensagens agressivas e com conteúdo impróprio, denuncie e/ou chame um adulto de confiança;
- Não esqueça dos esportes, da biblioteca e das brincadeiras sem computador.

# PERIGOS NA REDE

## CiberCrime - Crime Digital

Práticas criminosas utilizando meios eletrônicos como a Internet. Uso das novas tecnologias para ações ilícitas como roubo, chantagem, difamação, calúnia e violações aos Direitos Humanos fundamentais. O ciberespaço também é um espaço público que reflete a diversidade e complexidade da sociedade, tanto nas qualidades quanto na possibilidade de atos ilegais.

## Cuidado

- Como todo crime, prejudica as pessoas moralmente ou financeiramente;
- Quem quer praticar crimes pela Internet se aproveita da sensação de anonimato e de impunidade;
- Precisamos respeitar as leis também online para manter a Internet um espaço público aberto, livre e seguro;
- Falsa crença de que a Internet é uma terra sem lei, do "posso tudo e ninguém me acha"

## Dicas para manter-se Seguro

- Divulgue o mínimo de informações pessoais na Internet, seja discreto;
- Troque senhas com freqüência e evite utilizar senhas fáceis como datas;
- No trabalho ou na Lan House, não diga sua senha para ninguém nem deixe seu computador conectado ao se afastar da mesa;
- Não grave arquivos confidenciais ou dados pessoais em Lan Houses. Use pen drive ou CD e apague da área de trabalho os arquivos que abriu;
- Percebendo alguma irregularidade em seu extrato bancário ou cartão de crédito, comunique imediatamente ao seu banco ou operadora;
- Nas compras pela Internet, dê preferência para pagamentos com cartão de crédito ou boleto bancário e sempre procure empresas conhecidas e respeitadas;
- Sempre desconfie de ofertas mirabolantes. O "conto do bilhete premiado" já chegou à Internet;
- Veja mais dicas no www.safernet.org.br

# PERIGOS NA REDE

## CiberBullying

Você ou algum conhecido seu recebe constantemente mensagens no celular, e-mails, recados no blog ou no site de relacionamento com xingamentos, ofensas e humilhações? Isto é um caso de Ciberbullying, uma violência grave que não pode ser encarada como apenas uma brincadeirinha entre colegas. Se já foi vítima, saiba que você não tem culpa. Isso é ação de alguém mal educado e mal intencionado que deve ser responsabilizado.

## Cuidado

- Agressão anonima;
- Pode se prolongar por anos;
- Não envie nem repasse mensagens que agridam outras pessoas. Ao repassá-las, você também está agredindo;
- Você gostaria que fizessem com você?
- Nem todo mundo consegue superar o trauma de uma violência como esta que deixa marcas para sempre.

## Dicas para manter-se Seguro

- Conte a algum adulto de confiança;
- Não responda e grave todas as mensagens e/ou imagens;
- Bloqueie o contato dos agressores no celular, chat, e-mail e redes de relacionamento;
- Mais dicas e orientações em www.safernet.org.br
- Seja sempre educado no que fizer pela Internet, cuidado com o que escreve e com as imagens que divulga;
- Se algum conhecido está sendo vítima, encoraje-o a denunciar e ajude-o;
- Muitos jovens já foram obrigados a pagar multas por terem ofendido colegas ou professores na Internet;
- O futuro da Internet depende do que fazemos com ela hoje. Ao usar a Internet para agredir e humilhar alguém, estimulamos novas leis de controle e proibição;
- Para manter a Internet livre e aberta amanhã, precisamos usá-la com respeito e ética hoje.

# PERIGOS NA REDE

## Sexting

O Sexting é uma palavra originada da união de duas palavras em inglês: sex (sexo) + texting (envio de mensagens). O Sexting descreve um fenômeno recente no qual adolescentes e jovens usam seus celulares, câmeras fotográficas, contas de email, salas de bate-papo, comunicadores instantâneos e sites de relacionamento para produzir e enviar fotos sensuais de seu corpo (nu ou seminu). Envolve também mensagens de texto eróticas (no celular ou Internet) com convites e insinuações sexuais para namorado(a), pretendentes e/ou amigos(as).

## Cuidado

- Infelizmente não são apenas nossos amigos que podem ter acesso ao que divulgamos online;
- Atuais e futuros colegas de escola e de trabalho, parentes, inimigos, estranhos e até criminosos podem ver, copiar e manipular o que você divulga na Internet para, no futuro, usar isso contra você;
- Uma vez online, perdemos completamente o controle da foto ou texto que publicamos;
- Podem parecer brincadeiras inocentes, mas este tipo de mensagem sensual coloca nossa privacidade em risco;
- Estas fotos podem dizer muito sobre sua vida para pessoas que você nem gostaria de conhecer;

## Dicas para manter-se Seguro

- Jamais se deixe levar por pressões para produzir ou publicar imagens sensuais;
- Tudo o que fazemos online tem conseqüências também fora da Internet. Pense muito bem antes de publicar;
- Quando tiver dúvidas em relação aos comportamentos sexuais, procure conversar com seus pais e amigos(as) de confiança antes de se expor pela Internet;
- Não há nada de errado em falar e discutir sobre sexualidade. O erro é não se proteger e não se informar sobre como manter relações saudáveis dentro e fora do ciberespaço;
- Proteja seus direitos sexuais e não facilite agressões;
- Pais: dialoguem com seus filhos para conhecer o que fazem online e orientá-los. Os valores e limites de sua família precisam ser discutidos também em relação aos comportamentos online. Converse com seus filhos sobre as noções de privacidade e de comportamento de risco para construir limites como proteção e não como proibição;
- Pais e educadores: Saiba que você não precisa ser expert em tecnologia, basta transpor a cidadania também para este novo ciber-espaço público;

# PERIGOS NA REDE

## Chantagem On-Line

Você ou algum conhecido seu recebe ou recebeu mensagens no celular, e-mails, recados no Blog ou no site de relacionamento com convites para encontro, imagens de sexo ou conteúdos impróprios para sua idade? Isto pode ser uma tentativa de aliciamento. Infelizmente, na Internet, também há pessoas mal intencionadas que buscam vítimas para abusar e até mesmo sequestrar. Tome sempre muito cuidado para aproveitar a Internet sem correr este risco. Saiba como:

## Cuidado

- Os aliciadores fingem ser amigos virtuais, são "amáveis" nas primeiras conversas de Chat e Comunicador Instanâneo (MSN...);
- Se passam por crianças e conhecem o mundo infantil;
- Alguns se apresentam como adultos e enviam cenas de sexo com desenhos estimular fantasias impróprias;
- Elogiam demais para ganhar confiança e pedir informações como nome de escola, endereço, celular e fotos;
- Pedem cada vez mais fotos até solicitar conversas com webcam;
- Manipulam fotos e colocam o rosto da vítima em cenas de sexo;
- Ameaçam divulgar na Internet as fotos manipuladas para humilhar a vítima diante de amigos e familiares em sites;
- Ameaçam saber o endereço para agredir presencialmente em casa ou na escola;
- Nos piores casos, podem terminar em sequestro e abuso sexual das vítimas.

## Dicas para manter-se Seguro

- Cuidado, nunca teremos certeza de quem está por trás de um perfil, de um e-mail ou apelido;
- Não responda as mensagens de desconhecidos e grave quando houver ameaça ou imagens violentas;
- Jamais aceite convite para encontrar presencialmente um amigo virtual sem autorização. Mesmo com os responsáveis, vá a local público;
- Bloqueie o contato dos agressores no celular, chat, e-mail e redes de relacionamento;
- Se algum conhecido está sendo vítima, encoraje-o a denunciar e ajude-o a buscar apoio;
- Quando o conteúdo envolve crianças e adolescentes na Internet, você pode denunciar em www.denuncie.org.br , ligar no Disque 100, ir a uma delegacia especializada ou se dirigir ao Conselho Tutelar mais próximo;
- Lembre-se que, somente denunciando às autoridades, é que os criminosos poderão ser punidos. Jamais tente fazer justiça com as próprias mãos.

# PERIGOS NA REDE

## Roubo de Dados

Tomar e/ou utilizar os dados pessoais como senha, perfil, comunidade, avatar, personagem ou e-mail de um usuário sem a autorização ou consentimento para qualquer fim pode ser considerada crime.

## Cuidado

- Invasão da privacidade;
- Atitude contra as leis vigentes no País, portanto pode ser crime;
- Gera insegurança e constrangimento para os internautas;
- Se passar por outra pessoa na Internet para ofender e humilhar também é crime.

## Dicas para manter-se Seguro

- Não abrir arquivos anexos compactados (por exemplo, com extensão .ZIP) de remetente desconhecido;
- Não instalar programas que sejam enviados por e-mail de desconhecidos. Estes podem invadir seu computador e roubar tudo;
- Manter o anti-vírus e firewall sempre atualizados;
- Os navegadores de Internet livres como o Mozilla Firefox podem ser mais seguros;
- Não acredite em todas as informações que receber ;
- Esteja sempre em alerta, não adicione pessoas que você não conhece e suspeite de e-mails desconhecidos;
- Informação é a base de tudo, portanto, esteja sempre atualizado sobre os cuidados quanto à utilização segura da Internet;
- Desconfie de anexos sem comentários no corpo do e-mail.
- Denuncie perfis falsos e páginas que agridam você ou seus amigos;
- Se precisar solicitar retirada de conteúdo falso que te ofenda na Internet, veja orientações em: www.safernet.org.br/site/prevencao/orientacao.

# PERIGOS NA REDE

## Vírus

São programas de computador criados com intenção maliciosa, como roubar dados, danificar ou invadir sistemas. Mesmo sem percebermos, eles se espalham para infectar os computadores por meio de e-mail, troca de arquivos e programas. Por terem a capacidade de se automultiplicar, como as doenças nos seres vivos, esses programas receberam o apelido de vírus.

## Cuidado

- São instalados e funcionam sem que o usuário perceba;
- Estão por todos os lados na Internet e sempre se " atualizam" com os novos programas;
- Podem roubar senhas e apagar todas as informações preciosas de seu computador.

## Dicas para manter-se Seguro

- Use anti-vírus e atualize seus programas para ter sempre os "novos remédios";
- Lembre de usar seu anti-vírus semanalmente para fazer sempre um "check-up";
- Não abra e-mail nem arquivos de estranhos;
- Não abra programas ou fotos que dizem oferecer prêmios;
- Cuidado com os e-mails falsos de bancos, lojas e cartões de crédito;
- Jamais abra arquivos que terminem com: PIF, SCR, BAT, VBS. Atenção especial com os EXE e COM;
- Os Softwares Livres costumam ser mais seguros contra vírus.

# PERIGOS NA REDE

## Invasão

Ocorre quando alguém entra no computador de outra pessoa sem autorização para roubar dados, criar falsas mensagens e danificar os programas. O invasor pode estar em qualquer lugar do mundo e invadir seu computador ou sua rede.

## Cuidado

- É um tipo de cibercrime;
- Quanto mais informações publicar, maior o seu risco;
- Delete as correntes de e-mails, não encaminhe e não responda essas mensagens;
- É um crime transnacional, ou seja, envolve vítimas e criminosos de vários países ao mesmo tempo, sem limites de fronteira;

## Dicas para manter-se Seguro

- Evite abrir arquivos de desconhecidos seja no e-mail, chat, comunicador intantâneo ou redes de compartilhamento;
- Troque suas senhas periodicamente;
- Atualize sempre seu anti-vírus;
- Os navegadores de Internet livres, como o Mozilla Firefox, costumam ser mais seguros;
- Não podemos acreditar em tudo e nem em todos online;
- Cuidado, este tipo de crime está chegando rapidamente aos celulares, mp3 players e às TV's e todos aparelhos que estejam conectados à Internet.
- Confira mais dicas em www.safernet.org.br/prevencao

# PERIGOS NA REDE

## Justiceiros Virtuais

Algumas pessoas tentam "fazer justiça" com as próprias mãos, invadindo sites para tirar alguns conteúdos da Internet. Em vez de buscarem os meios legais para resolver o problema, tentam solucioná-lo por conta própria e quase sempre dificultam os trabalhos de investigação das autoridades. Além disso, se colocam em risco ao desafiar criminososperigosos.

## Cuidado

- Iludem e seduzem jovens internautas para serem "heróis na Internet";
- Muitas vezes comentem crimes para combater outros crimes;
- Podemcolocarpessoasem risco sem que elas se dêem conta da gravidade do problema;
- Entram em disputa direta com redes de pessoas perigosas;
- Alguns usam ameaças e chantagem para manter pessoas "presas" aos grupo.

## Dicas para manter-se Seguro

- Cuidado com as comunidades ou usuários que se consideram heróis da Internet, detetives digitais ou ciberpoliciais;
- Não faça justiça com o seu próprio mouse;
- Lembre-se de que todos tem direito de se expressar livremente, respeitando as leis e os Direitos Humanos;
- Se for ameaçado, comunique imediatamente aos seus familiares, à polícia e denuncie;
- Se algum conhecido está envolvido com justiceiros virtuais, esclareça sobre os riscos e oriente-o a comunicar às autoridades em caso de ameaças ou intimidações;
- Para transformar a Internet em um espaço mais seguro e legal, seja educado e denuncie quando presenciar algo suspeito;
- Em caso de roubo, difamação e fraude, procure uma delegacia especializada em crimes eletrônicos;
- Em caso de visualizar conteúdos com cenas de violência contra crianças, racismo, intolerância de gênero ou religiosa, denuncie em www.denuncie.org.br;
- Saiba mais sobre o trabalho das autoridades brasileiras através do Site da Polícia Federal www.dpf.gov.br, do Ministério Público Federal www.mpf.gov.br e dos Ministérios Públicos e Polícias de seu estado.
- Mais dicas em www.safernet.org.br/prevencao

# Software Livre

A Central Nacional de Denúncias de Crimes Cibernéticos, um dos principais projetos da SaferNet Brasil, possui um sistema automatizado de gestão de denúncias, que permite ao internauta acompanhar, em tempo real, cada passo do andamento do seu registro. O sistema, único na América Latina e Caribe, foi desenvolvido pela equipe de TI (Tecnologia da Informação), baseado em Software Livre.

**Por que Software Livre?**

A SaferNet Brasil compartilha da ideologia da rede de Software Livre, que defende a liberdade do usuário para executar, distribuir, modificar e repassar as alterações, sem depender de permissão do autor do programa. Para nós é fundamental ter o direito de conhecer plenamente o funcionamento de cada programa utilizado.

Para entender este conceito, você deve pensar em liberdade, ou melhor, em pelo menos quatro liberdades que são asseguradas aos usuários. Elas foram estabelecidas pela Free Software Foundation (www.fsf.org) como os requisitos mínimos para que um software seja considerado livre. São elas:

- A liberdade de executar o programa, para qualquer propósito;
- A liberdade de estudar como o programa funciona, e adaptá-lo para as suas necessidades;
- A liberdade de redistribuir cópias de modo que você possa beneficiar o próximo;
- A liberdade de aperfeiçoar o programa, e liberar os seus aperfeiçoamentos, de modo que toda a comunidade se beneficie.

Para que o usuário possa usufruir de algumas dessas liberdades (como a liberdade de estudar o programa e a liberdade de modificá-lo), é necessário acesso ao código-fonte.

Código-fonte é uma das etapas da criação de um programa de computador. É nele onde o programador escreve, passo a passo, as instruções que o software deverá executar. O importante é que, no código-fonte, essas instruções estão escritas de forma que os seres humanos possam compreender, enquanto que o arquivo executável (o programa em si) não pode ser compreendido pelas pessoas, por estar em linguagem binária. Os distribuidores de software não-livre entregam ao usuário apenas o executável, impedindo o usuário de estudar como o programa funciona e modificá-lo.

Note que em nenhum dos itens se fala de preços ou custos. É um erro comum achar que Software Livre é software gratuito. É verdade, sim, que a maioria dos Softwares Livres é distribuída gratuitamente, mas essa é uma conseqüência esperada da terceira e da quarta liberdades, que permitem distribuir o programa com ou sem modificações, sem restrições.

O Software Livre pode ser usado em qualquer tipo de sistema computacional para qualquer tipo de trabalho ou atividade, sem que seja necessário comunicar ao desenvolvedor ou a qualquer outra entidade em especial. O sistema operacional GNU/Linux e o navegador Firefox são os exemplos mais conhecidos de Softwares Livres.

Benefícios para os usuários:

- Poder utilizar o software para qualquer finalidade;
- Ter acesso ao código fonte e poder modificá-lo, sem restrições;
- Poder copiá-lo e executá-lo em quantas máquinas desejar (o software não-livre, em geral, impõe restrições quanto a isso);
- Poder distribuí-lo;
- Contar com estabilidade, seguranças, e correções de falhas de forma ágil;
- Ter o computador equipado com software de qualidade a um custo baixo ou nulo;
- Não depender das restrições impostas pelas licenças de softwares proprietários e de preços abusivos das novas versões;
- Não depender de apenas um fornecedor;
- Ficar livre da pirataria e ter todo o seu software legalizado;
- Incentivar o desenvolvimento de tecnologia local;
- Interagir e compartilhar soluções com comunidades, sejam físicas ou virtuais;
- Lutar contra o monopólio de grandes corporações que tentam se apropriar do conhecimento intelectual coletivo para benefício privado.

Para a SaferNet Brasil, utilizar Software Livre é a única maneira de assegurar a continuidade dos programas utilizados, garantir que os programas poderão ser adaptados às necessidades particulares da organização, e ter certeza que o programa faz aquilo que esperamos que ele faça, sem rotinas desconhecidas ou comportamentos inesperados.

Fontes: www.softwarelivre.org e www.psl-ba.softwarelivre.org

# Créditos

Esta cartilha foi elaborada pela equipe da SaferNet Brasil com o propósito de contribuir para o uso seguro e responsável da Internet brasileira.



Participaram deste projeto:

Ilustrações e design: Bruno Aziz

Equipe SaferNet:

- Diretor Presidente: Thiago Tavares
- Diretor de Prevenção: Rodrigo Nejm
- Diretor de Tecnologia: Leandro Nunes
- Desenvolvedor de software e webdesigner: Aurélio A. Heckert
- Assessoria de Comunicação: Lenina Uzeda
- Desenvolvedor de software: Caio SBA
- Analista de Conteúdo: Ivã Coelho
- Desenvolvedor de software (estagiário): Daniel Cunha
- Desenvolvedor de software (estagiário): Caio Tiago Sousa
- Desenvolvedor de software (estagiário): Aline Bessa

Contamos também com o apoio de informações da cartilha Diálogo Virtual 1.1, criada por alunos do Curso Hackerteen em cooperação com a equipe da SaferNet Brasil.

Confira a versão para download no site **www.SaferNet.org.br**

Sinta-se à vontade para usá-la e divulgá-la!

Obrigado por também compartilhar do ideal de Internet segura e ética!

www.SaferNet.org.b r/cartilha

**Comemoração**

**Realização**

**Cooperação**

Secretaria Especial
dos Direitos Humanos